Proposed Amendment for U.S. Patent Application Serial No. 09/874,574
K&S File No. 05456.105035
Examiner Nalven // Group Art Unit 2134
For Telephonic Interview of Wednesday, February 9, 2005 @ 2:00PM EST
For Discussion Purposes Only
Applicant Representative's Phone Number (Steve Wigmore, Reg. No. 40,447): (404)572-2884

Independent Claims Only

1. A computer-implemented method comprising:

detecting a data signature by evaluating communications at an application layer level between a target and a suspect; [[and]]

correlating said data signature with an application layer fingerprint of the target to determine to what extent said target is vulnerable to said data signature; and

evaluating contextual information related to the data signature to determine a likelihood that said target is under attack, the contextual information comprising at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature.

14. A computer-implemented method comprising:

identifying a data signature encapsulated in an application layer data field and directed at a target using an application layer protocol;

evaluating ~~said~~ a context of the data signature[['s]] ~~context~~ by one of:

comparing the data signature to the application layer data field;

comparing the data signature to the application layer protocol; and

determining whether said data signature poses a threat based on said context of said data signature.

25. A computer-implemented method comprising:

monitoring a plurality of data transmissions at an applications layer level between a suspect and a target to identify one or more data signatures, said data transmissions indicating a current state of communication between said suspect and said target;

evaluating contextual information related to each data signature, the contextual information comprising at least one of an application layer data field type used to encapsulate a respective data signature and an application layer protocol type used to transmit a respective data signature; and

evaluating a likelihood that said target is under attack based on the contextual information of one or more data signatures of said transmissions and said current state of communication.

37. A machine-readable medium having program code stored thereon which, when executed by a machine, causes said machine to perform the operations of:

detecting a data signature by evaluating communications at an application layer level between a target and a suspect; [[and]]

correlating said data signature with a fingerprint of thc target to determine to what extent said target is vulnerable to said data signature; and

evaluating contextual information related to the data signature to determine a likelihood that said target is under attack, the contextual information comprising at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature.

50. A machine-readable medium having program code stored thereon which, when executed by a machine, causes said machine to perform the operations of:

identifying a data signature encapsulated in an application layer data field directed at a target using an application layer protocol;

evaluating ~~said~~ a context of the data signature[['s]] ~~context~~ by one of:

comparing the data signature to the application layer data field;

comparing the data signature to the application layer protocol; and

determining whether said data signature poses a threat based on said context of said data signature.

56. A machine-readable medium having program code stored thereon which, when executed by a machine, causes said machine to perform the operations of:

monitoring a plurality of data transmissions at an applications layer level between a suspect and a target to identify one or more data signatures, said data transmissions indicating a current state of communication between said suspect and said target;

evaluating contextual information related to each data signature, the contextual information comprising at least one of an application layer data field type used to encapsulate a respective data signature and an application layer protocol type used to transmit a respective data signature; and

evaluating a likelihood that said target is under attack based on the contextual information of one or more data signatures of said transmissions and said current state of communication.